HIP Working Group
Internet-Draft
Intended status: Experimental
Expires: July 30, 2010

A. Keranen
Ericsson
January 26, 2010

Host Identity Protocol Signaling Message Transport Modes
draft-keranen-hip-over-hip-00.txt

Abstract

This document specifies two transport modes for Host Identity Protocol signaling messages that allow conveying them over encrypted connections initiated with the Host Identity Protocol.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Host Identity Protocol [RFC5201] signaling messages can be exchanged over plain IP using the protocol number reserved for this purpose, or over UDP using the UDP port reserved for HIP NAT traversal [I-D.ietf-hip-nat-traversal]. When two hosts perform a HIP base exchange, they set up an encrypted connection between them for data traffic, but continue to use plain IP or UDP for HIP signaling messages.

This document defines how the encrypted connection can be used also for HIP signaling messages. Two different modes are defined: HIP over Encapsulating Security Payload (ESP) and HIP over TCP. The benefit of sending HIP messages over ESP is that all signaling traffic (including HIP headers) will be encrypted. If HIP messages are sent over TCP (which in turn is transported over ESP), TCP can handle also message fragmentation where needed.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Protocol Extensions

This section defines how support for different HIP signaling message transport modes is negotiated and the normative behavior required by the extension.

3.1. Mode Negotiation in HIP Base Exchange

A HIP host implementing this specification SHOULD indicate the modes it supports, and is willing to use, in the base exchange. The HIP signaling message transport mode negotiation is similar to HIP NAT traversal mode negotiation: first the Responder lists the supported modes in a HIP_TRANSPORT_MODE parameter (see Figure 1) in the R1 packet. If the Initiator supports, and is willing to use, any of the modes proposed by the Responder, it selects one of the modes by adding a HIP_TRANSPORT_MODE parameter containing the selected mode to the I2 packet. Finally, if the Initiator selected one of the modes and the base exchange succeeds, hosts use the selected mode for the following HIP signaling messages sent between them.

```
       0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |             Type              |             Length            |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |           Mode ID #1          |           Mode ID #2          |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |           Mode ID #n          |             Padding           |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type   [TBD by IANA; 990]
Length   length in octets, excluding Type, Length, and padding
Mode ID   defines the proposed or selected transport mode(s)

The following mode IDs are defined:

ID name	Value
RESERVED	0
ESP	1
ESP-TCP	2

Figure 1: Format of the HIP_TRANSPORT_MODE parameter

3.2. HIP Messages on Encrypted Connections

If the ESP mode is selected in the base exchange, both hosts MUST listen for incoming HIP signaling messages and send outgoing messages on the encrypted connection. The ESP header's next header value for such messages MUST be set to HIP (139).

If the ESP-TCP mode is selected, the Responder MUST start to listen for an incoming TCP connection on the port 10500 on the encrypted connection and the Initiator MUST create a TCP connection to the Responder on the same port. The Initiator SHOULD use port 10500 as the source port for the TCP connection. Once the TCP connection is established, both hosts MUST listen for incoming HIP signaling messages and send the outgoing messages using the TCP connection. The ESP next header value for messages sent using the ESP-TCP mode connections MUST be set to TCP (6).

Since TCP provides reliable transport, the HIP messages sent over TCP MUST NOT be retransmitted for the purpose of achieving reliable transmission. Instead, a host simply waits for the same time that would be taken by the maximum amount of retransmissions with unreliable transmission before concluding that there is no response.

4. Security Considerations

By exchanging the HIP messages over ESP connection, all HIP signaling data (after the base exchange) will be encrypted, but only if NULL encryption is not used. Thus, host requiring confidentiality for the HIP signaling messages must check that encryption is negotiated to be used on the ESP connection.

5. Acknowledgements

Thanks to Gonzalo Camarillo for comments on the draft.

6. IANA Considerations

This section is to be interpreted according to [RFC5226].

This document updates the IANA Registry for HIP Parameter Types [RFC5201] by assigning new HIP Parameter Type value for the HIP_TRANSPORT_MODE parameter (defined in Section 3.1).

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5201] Moskowitz, R., Nikander, P., Jokela, P., and T. Henderson, "Host Identity Protocol", RFC 5201, April 2008.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

7.2. Informational References

[I-D.ietf-hip-nat-traversal]
Komu, M., Henderson, T., Tschofenig, H., Melen, J., and A. Keranen, "Basic HIP Extensions for Traversal of Network Address Translators", draft-ietf-hip-nat-traversal-09 (work in progress), October 2009.

Author's Address

Ari Keranen
Ericsson
Hirsalantie 11
02420 Jorvas
Finland

Email: Ari.Keranen@ericsson.com